Security Plan Template for NASA Headquarters Major Applications and General Support Systems

SENSITIVE UPON COMPLETION

December 3, 1998

National Aeronautics and Space Administration
Office of Headquarters Operations
Information Technology and Communications Division

Directions

This template is for the development of a security plan for either a **major application** or **general support system**. Each section of this Plan has a description or definition of the information that is required, and should be rewritten or deleted as necessary. If a section or appendix is not applicable to a particular system or application, type: *This section is not applicable to this particular plan*, and leave the section heading as a 'place holder.'

Where applicable, tables have been added to show examples or assist in supplying the requested information. The tables will also be helpful if the plan is being written about more than one system or application.

The body of this security plan is divided into the following sections:

Section 1 - Introduction *Section 2* - System/Application Information *Section 3* - Management Controls	Use for both Major Applications and General Support Systems.
Section 4 - Major Application *Section 5* - General Support System	Use Section 4 for a major application, and Section 5 for a general support system. Delete the unused section. When used for a General Support System, renumber the sections appropriately.

The security plan, at a minimum, should be marked, handled, and controlled as a sensitive document.

Delete this page when developing a security plan for an application or system.

I. Executive Summary

The objective of this security plan is to improve protection of information and Information Technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in this security plan. The completion of a security plan is a requirement of the Office of Management an Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, and Public Law 100-235, *Computer Security Act of 1987*. This document implements the above stated requirements using guidelines established by the National Institute of Standards and Technology (NIST), and also by the *NASA Procedures and Guidelines for the Security of Information Technology* (NPG 2810, Draft).

The purpose of this security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan also delineates responsibilities and expected behavior of all individuals who access the system. It provides managers and network administrators with a flexible, streamlined approach to protecting NASA Headquarters' *major applications* and *general support systems* that contain sensitive but unclassified information.

In order for the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risks.

Management authorization should be based on an assessment of various management, operational, security, and technical controls. As the security plan documents these types of controls, it should form the basis for the authorization, supplemented by more specific studies as needed.

A periodic review of controls should also contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

Appendix F, Planned / Recommended Items, contains a compiled list of the *planned* items found throughout this document, and of the items that require attention.

Security Plan Template for NASA Headquarters
Major Applications and General Support Systems

Table of Contents

1. Introduction

Today’s rapidly changing technical environment requires that a minimum set of management controls be in place to protect information technology (IT) resources. These management controls are directed at individual information technology users in order to reflect the distributed nature of today’s technology. Technical and operational controls support management controls. To be effective, these controls all must interrelate. This document describes the management, technical, and operational controls for NASA’s automated information systems.

Appendix A contains terms that are used in connection with a security plan.

1.1 Purpose

The purpose of this security plan is to:

- Provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; and

- Delineate responsibilities and expected behavior of all individuals who access the system.

1.2 Security Plan Responsibility

The System Owner[1] is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional *end users*, Information Owners[2], the System Administrator, and the System Security Manager.

Agencies may require contractor compliance with this guide as a contract requirement. A security plan in the format specified in this document is suggested in those cases where vendors are operating a system under contract to the federal government. In those instances where a contractor or other entity (e.g., state or local government) operates a system that supports a federal function, a security plan is required.

OMB Circular A-130 requires a summary of the security plan to be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35). Agencies should develop policy on the security planning process. Security plans are living documents that require periodic reviews, modifications, and milestone or completion dates for planned controls. Procedures should be in place outlining who reviews the plans and follows-up on planned controls. In addition, procedures are needed describing how security plans complete the authorization for processing process.

[1] The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners.

[2] The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The Information Owner retains that responsibility even when the data/information are shared with other organizations.

2. System/Application Information

This section provides information that applies to the particular major application or to the general support system. Both types of plans must contain general descriptive information regarding who is responsible for the system/application, the purpose of the system/application, and the sensitivity level of the system/application.

2.1 System/Application Name and Title

Each system/application should be assigned a unique name/identifier. Assigning a unique identifier to each system/application helps to ensure that appropriate security requirements, based on the unique requirements for the system/application, are met and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act).

The identifier could be a combination of alphabetic and numeric characters and can be used in combination with the system/application name. The unique name/identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time. In this section, list the unique name/identifier for the system/application.

2.2 Responsible Organization

The plan begins with listing the federal organizational sub-component responsible for the system. If a contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Identify the division and branch that operate or own the system. Include physical locations and addresses.

Example of Responsible Organization

National Aeronautics and Space Administration
Office of Security Administration
Room 1111
300 E Street SW
Washington, D.C. 20024

This system/application is maintained by:

Contractor Firm
409 3rd Street SW
Washington, D.C. 20024

2.3 Information Contact(s)

List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system/application. One of the contacts given should be identified as the system/application owner. The designated persons should have sufficient knowledge of the system/application to be able to provide additional information or points of contact, as needed.

Example Information Contacts

Ms. Jane Smith (system/application Owner)
ABC Division Chief
Street Address, Room
Washington, DC
(202) Number

Mr. Thomas Jones
Systems Administrator
Street Address
Washington, DC
(202) Number

Mr. John Doe
Program Manager
ABC Division
Street Address, Room
Washington, DC
(202) Number

2.4 Assignment of Security Responsibility

An individual must be assigned responsibility in writing to ensure that the major application or general support system has adequate security. To be effective, this individual should be knowledgeable of the management, operational, and technical controls used to protect the system/application.

Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system/application and who will act as the Automated Information System Security Officer (AISSO). Indicate whether the individual has been designated in writing as the AISSO.

Example Security Official

Bill Smith, AISSO
Computer Specialist
ABC Division, ZYZ Branch
Street Address
Washington, DC
(202) Number

2.5 System Operational Status

Indicate one of the following for the system's operational status.

- *Operational* — the system is operating.
- *Under development* — the system is being designed, developed, or implemented.
- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan.

2.6 Information Category

Identify the information category, as referenced in Section 4.2.9 of *the NASA Procedures and Guidance for the Security of Information Technology* (NPG 2810, Draft). Categories to choose includes:

- Mission (MSN);
- Business and Restricted Technology (BRT);
- Scientific, Engineering, and Research (SER);
- Administrative (ADM); or
- Public Awareness (PUB).

2.7 General Description/Purpose

Present a brief description (one-three paragraphs) of the function and purpose of the system/application. Include the following types of information in the description:

- Make and model number;

- Major uses or functions (such as, modeling, simulations, accounting, analysis);

- Network access and connectivity;

- System software and versions and the software applications running on the system;

- Operated by Government or contractors (owned or leased);

- Hours of operation;

- Critical processing periods (for example, end of month, pay day, etc.);

- Indicate whether the system serves a large number of off-site users (such as university students, other agencies, or foreign nationals); and

- Number of user accounts.

2.8 System Environment

Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet).

- Describe controls used to protect communication lines in the appropriate sections of the security plan;

- The system is connected to the Internet;

- It is located in a harsh or overseas environment;

- Software is rapidly implemented;

- The software resides on an open network used by the general public or with overseas access;

- The application is processed at a facility outside of the agency's control; or

- The general support mainframe has dial-up lines.

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

Example System Environment

The system is physically housed in a government-owned building located in Washington, D.C. The entire building is occupied by the National Aeronautics and Space Administration (NASA) and contractor personnel and is not open to the general public. The system uses mainframe hardware. The system consists of a Brand X 9999 supercomputer and a Brand Y 8888 mainframe configuration. The operating system running on the Brand X 9999 system is OS-YYYY and on the Brand Y 8888 system is OS-OOOO1. The security software protecting all system resources from the top levels are XYZ and PDQ. DOA-XX-0123, a complex wide area communication network system, provides support to client agencies nationwide.

2.9 System Interconnection/Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those risks. The security plan for the systems often serves as a mechanism to effect this security information exchange and allow management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization should detail the rules of behavior and controls that must be maintained by the interconnecting systems. A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan. Refer to the section on Rules of Behavior.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- List of interconnected systems (including Internet);

- Unique system identifiers, if appropriate;

- Name of system(s);

- Organization owning the other system(s);

- Type of interconnection (TCP/IP, Dial, SNA, etc.);

- Short discussion of major concerns or considerations in determining interconnection (do not repeat the system rules included in the section on Rules of Behavior);

- Name and title of authorizing management official(s);

- Date of authorization;

- System of Record, if applicable (Privacy Act data);

- Sensitivity level of each system;

- Interaction among systems; and

- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system.

2.10 Sensitivity of Information Handled

This section provides a description of the types of information handled by the system and an analysis of the criticality of the information. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and one of the major factors in risk management. The description will provide information to a variety of users, including:

- Analysts/programmers who will use it to help design appropriate security controls;
- Internal and external auditors evaluating system security measures; and
- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws and regulations affecting the system and a general description of sensitivity as discussed below.

2.11 Laws, Regulations, and Policies Affecting the System

List any laws or regulations that establish specific requirements for **confidentiality**, **integrity**, or **availability** of data/information in the system. The Computer Security Act of 1987, OMB Circular A-130, and agency AIS security requirements need not be listed since they mandate security for all systems. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). **Appendix B** contains various types of policy and definitions.

Example of Applicable Laws, Regulations, and Policies Affecting the System

Privacy Act of 1974 (PL-93-579)
Paperwork Reduction Act of 1980 as amended in 1995
OMB Circular A-123

2.12 General Description of Sensitivity

Both information and information systems have distinct life-cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for **confidentiality**, **integrity**, **and availability** of the information. This process should occur at the beginning of the information system's life-cycle and be re-examined during each life-cycle stage.

The integration of security considerations early in the life-cycle avoids costly retrofitting of safeguards. However, security requirements can be incorporated during any life-cycle stage. The purpose of this section is to review the system requirements against the need for availability, integrity, and confidentiality. By performing this analysis the value of the system can be determined. The value is one of the first major factors in risk management. A system may need protection for one or more of the following reasons:

- *Confidentiality*

The system contains information that requires protection from unauthorized disclosure.

Example of Information Requiring Protection — Confidentiality

Timed dissemination information (e.g., crop report information), personal information (covered by Privacy Act), proprietary business information (e.g., business plans).

- *Integrity*

The system contains information, which must be protected from unauthorized, unanticipated, or unintentional modification.

Example of Information Requiring Protection — Integrity

Census information, economic indicators, or financial transaction systems.

- *Availability*

The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Example of Information Requiring Protection — Availability

Systems critical to safety, life support, and hurricane forecasting.

Describe, in general terms, the information handled by the system and the need for protective measures.

- Relate the information handled to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability**).

- Include a statement of the estimated risk and magnitude of harm resulting from the , or unauthorized access to or modification of information in the system. To the extent possible, describe this impact in terms of cost, inability to carry out mandated functions, timeliness, etc.

For each of the three categories (**confidentiality**, **integrity**, and **availability**), indicate if the protection requirement is:

- *High* — a critical concern of the system;

- *Medium*— an important concern, but not necessarily paramount in the organization's priorities; or

- *Low* — some minimal level or security is required, but not to the same degree as the previous two categories.

Examples of a General Protection Requirement Statement

A high degree of security for the system is considered mandatory to protect the confidentiality, integrity, and availability. The protection requirements for all applications are critical concerns for the system.

or

Confidentiality is not a concern for this system as it contains information intended for immediate release to the general public concerning severe storms. The integrity of the information, however, is extremely important to ensure that the most accurate information is provided to the public to allow them to make decisions about the safety of their families and property. The most critical concern is to ensure that the system is available at all times to acquire, process, and provide warning information immediately about life threatening storms.

Example Confidentiality Considerations	
Evaluation	**Comment**
High	The application contains proprietary business information and other financial information, which, if disclosed to unauthorized sources, could cause unfair advantage for vendors, contractors or individuals and could result in financial loss or adverse legal action to user organizations.
Medium	Security requirements for assuring confidentiality are of moderate importance. Having access to only small portions of the information has little practical purpose and the satellite imagery data does not reveal information involving national security.
Low	The mission of this system is to produce local weather forecast information that is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.

Example Integrity Considerations	
Evaluation	**Comment**
High	The application is a financial transaction system. Unauthorized or unintentional modification of this information could result in fraud, under-or-over payments of obligations, fines or penalties resulting from late or inadequate payments, and loss of public confidence.
Medium	Assurance of the integrity of the information is required to the extent that destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.
Low	The system mainly contains messages and reports. If these messages and reports were modified, by unauthorized, unanticipated or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization.

Example Availability Considerations	
Evaluation	**Comment**
High	The application contains personnel and payroll information concerning employees of the various user groups. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.
Medium	Information availability is of moderate concern to the mission. Macintosh and IBM PC availability would be required within the 4 to 5 day range. Information backups maintained at off-site storage would be sufficient to carry on with limited office tasks.
Low	The system serves primarily as a server for E-mail for the seven users of the system. Conference messages are duplicated between Seattle and D.C. servers. Should the system become unavailable, the D.C. users would connect to the Seattle server and continue to work with only the loss of old mail messages.

As described in NPG 2810 (Draft), if this Plan is for a General Support System that has been identified as needing *special management attention*, select one of the following and describe the reasons why *special management attention* is required:

1. Major Information System - a system that has been designated by the Chief Information Officer (CIO) as a major information system for OMB A-11 reporting.

2. Mission Critical System - a system that provides agency wide support, such as a wide area network, agency wide business function, command and control of space system, agency wide consolidated computer resource, or computer resource that affects life support.

3. National Resource Protection (NRP) Facility - a computer resource that is critical to a facility or operation as designated under the NRP program by the cognizant Program Office (reference NASA Policy Directive 1600.2, NASA Security Program).

4. Center Designated - other computer systems that the Center Director or CIO has designated as requiring special management attention.

2.13 Impact of Loss

Describe the potential impacts if the system, application, or the information processed is altered, destroyed, or unavailable (that is, at what point does the loss become a high priority - 1 hour, 1 day, 1 week, or 1 month?).

Discuss the loss of data, loss of processing time, recovery cost for hardware and software (i.e., programs), impact to budgets, impact to customers, and estimated recovery time.

2.14 System Value

Estimate the replacement cost for the hardware and software programs that comprise the system. Include the cost of rebuilding databases and programming code if they are not backed up or they are not remotely located.

3. Management Controls

Describe the management control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application or general support system. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system. A brief explanation of the various management controls is provided.

3.1 Risk Assessment and Management

OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should be described. For example, did the selected risk assessment methodology identify threats, vulnerabilities, and the additional security measures required to mitigate or eliminate the potential that those threats/vulnerabilities could have on the system or its assets? Include the date that the system risk assessment was conducted, who conducted it, and who approved it. State how the identified risks relate to the requirements for confidentiality, integrity, and availability determined for the system.

If there is no risk assessment for your system, include a milestone date (month and year) for completion of the risk assessment. If the risk assessment is more than three years old or there have been major changes to the system or functions, include a milestone date (month and year) for completion of a new or updated risk assessment. Assessing the risk to a system should be an on going activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented.

3.2 Security Controls

OMB Circular A-130 requires that at least every three years an independent review of security controls for each major application be performed. For general support systems, OMB Circular A-130 requires that the security controls be reviewed by an independent audit or self review at least every three years. Describe the type of independent security review and findings conducted on the major application or general support system in the last three years. Include information about the last independent audit or review of the system and who conducted the review. Discuss any findings or recommendations from the review and include information concerning correction of any deficiencies or completion of any recommendations. Indicate if the review identified a deficiency reportable under OMB Circular No. A-123 or the Federal Managers' Financial Integrity Act. If a baseline requirement, or security feature was not activated, state why this was the case. Indicate in this section if an independent audit or review has not been conducted on this system.

Security reviews, assessments, or evaluations may be conducted on your system by internal or external organizations or groups. Such reviews include ones conducted on your facility or site by physical security specialists from other components of your organization, system audits, or security program reviews performed by your Inspector General's staff or contractors. These reviews may evaluate the security of the total system or a logical segment/subsystem. The system descriptions, findings, and recommendations from these types of reviews may serve as the independent review, if the review is thorough, and may provide information to support your risk assessment and risk management. If other types of security evaluations have been conducted on your system, include information about who performed the review, when the review was performed, the purpose of the review, the findings, and the actions taken as a result of the review.

The review or audit should be independent of the manager responsible for the major application or general support system. Independent audits can be internal or external but should be performed by an individual or organization free from personal and external factors which could impair their independence or their perceived independence (e.g., they designed the system under review). For some high-risk systems with rapidly changing technology, three years may be too long and reviews may need to be conducted more frequently. The objective of these reviews is to provide verification that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for the system. The determination that the level of risk is acceptable must be made relative to the system requirements for confidentiality, integrity, and availability as well as the identified threats.

The security of a system may degrade over time, as the technology changes, the system evolves, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing can assist in the on-going review of system security measures. These tools, however, are no substitute for a formal management review at least every three years.

3.3 Rules of Behavior

Attach the rules of behavior for the major application or general support system as an appendix and reference the appendix number in this section, or insert the rules into this section. A set of rules of behavior must be established for each system. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains. The acceptable level of risk should form the basis for determining the rules. **Appendix C** contains a sample rules of behavior for a financial system, which is categorized as a major application. **Appendix D** contains a sample rules of behavior for a local area network, which is categorized as a general support system.

The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or non-compliance. The rules should be in writing and form the basis for security awareness and training.

They shall also include appropriate limits on interconnections to other systems and define service provision and restoration priorities. The rules of behavior should cover such matters as:

- Process for obtaining an account;
- Process for accessing the system from home or while on travel;
- Type of information that may be stored on the system;
- User privileges and limitations;
- Dial-in access;
- Connection to the Internet;
- Use of copyrighted works;
- Unofficial use of government equipment;
- Assignment and limitation of system privileges, and individual accountability. Administrative and technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Such rules would also include limitations on changing information, searching databases, or divulging information;
- Process for restoring service from system crashes or maintenance;
- Process for escorting personnel who do not have access to the system; and
- Consequences for failure to follow the rules.

Rules of behavior may be enforced through administrative sanctions specifically related to the system (e.g., loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct.

The rules of behavior should be made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt.

3.4 Life-Cycle Security Planning

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. It is recognized that in some cases, the system may at any one time be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while the older, batch oriented input sub-system is being replaced by a new, distributed and interactive user interface. In this case, the life cycle phases for the system are the disposal phase (data and equipment) related to the retirement of the batch oriented transaction system, the initiation and acquisition phase associated with the replacement interactive input system, and the operations/maintenance phase for the balance of the system.

In this section, determine which phase(s) of the life cycle the system, or parts of the system, are in. Identify how security has been handled during the applicable life cycle phase. Listed below is a description of each phase of the life cycle, which includes questions that will prompt the reader to identify how security has been addressed during the life cycle phase(s) that the major application or general support system is in.

There are many models for the IT system life-cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

3.4.1 Initiation Phase

During the initiation phase, the need for a system is expressed and the purpose of the system is documented. A sensitivity assessment can be performed which looks at the sensitivity of the information to be processed and the system itself. If the system, or part of the system is in the initiation phase, reference the sensitivity assessment described in the section on Sensitivity of Information Handled.

3.4.2 Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, security requirements should be developed at the same time system planners define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). If the system or part of the system is in this phase, include a general description of any specifications that were used and whether they are being maintained. Address the following:

- During the system design, were security requirements identified?

- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?

- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?

- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?

- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

3.4.3 Implementation Phase

In the implementation phase, the system's security features should be configured and enabled, the system should be tested and installed or fielded, and the system authorized for processing. (Refer to the section on Authorize Processing for a description of that requirement). A design review and systems test should be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official agency records.

If the system or parts of the system are in the implementation phase, describe when and who conducted the design reviews and systems tests. Include information about additional design reviews and systems tests for any new controls added after the initial acceptance tests were completed. Discus whether the documentation of these reviews and tests have been kept up-to-date and maintained in the organization records.

3.4.4 Operation/Maintenance Phase

During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. In various sections of this security plan, the following high-level items should be documented:

- Security Operations and Administration. Operation of a system involves many security activities. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.

- Operational Assurance. Operational assurance examines whether a system is operated according to its current security requirements. This includes both the actions of people who operate or use the system and the functioning of technical controls. (Reference section on Authorize Processing for a description of that requirement).

- Audits and Monitoring. To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring.

3.4.5 Disposal Phase

The disposal phase of the IT system life-cycle involves the disposition of information, hardware, and software. Describe in this section how the following items are disposed:

- Information. Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their agency office responsible for retaining and archiving federal records.

- Media Sanitization. The removal of information from a storage medium (such as a hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.

3.4.6 Authorization to Process

The term "authorization to process" is the authorization granted by a management official for a system to process information. (*Note*: Some agencies refer to this authorization as accreditation.) Authorization provides a form of quality control and is required under OMB Circular A-130. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing processing in a system, a manager accepts the risk associated with it. In this section of the plan, include the date of authorization, name, and title of management official. This authorization can be a cover letter attached to the plan or a signed statement at the end of the document. This authorization must clearly state that the manager finds that the IT Security Plan adequately secures the system its data, and its operation. If not authorized, provide the name and title of manager requesting approval to operate and date of request.

Both the security official and the authorizing management official have security responsibilities. The security official is closer to the day-to-day operation of the system and will direct, perform, or monitor security tasks. The authorizing official will normally have general responsibility for the organization supported by the system. Authorization is not a decision that should be made by the security staff. Some agencies have established the system approval process as a formal accreditation procedure where the approving authority is termed the Designated Approving/Accreditation Authority (DAA). Normalization of the system authorization process reduces the potential that systems will be placed into a production environment without appropriate management review.

Management authorization must be based on an assessment of management, operational and technical controls. Since the security plan reports on the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by a technical evaluation and/or security evaluation, risk assessment, contingency plan, and signed rules of behavior. Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

Below is a list of some of the security controls that must be in place prior to authorizing a system for processing. The level of controls should be consistent with the level of sensitivity the system contains.

- Technical and / or security evaluation complete.
- Risk assessment conducted.
- Rules of behavior established and signed by users.
- Contingency plan developed and tested.
- Security plan developed, updated, and reviewed.
- Meets applicable federal laws, regulations, policies, guidelines, and standards.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.
- In-place safeguards are operating as intended.

4. Major Application Format

This portion of the Security Plan is for a major application, and is divided into two main sections, being Operational and Technical Controls.

4.1 Operational Controls

The operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise – and often rely upon management activities as well as technical controls.

Each of the following control sections should begin by indicating the appropriate ***Security Control Measure Status***, being, **in place** or **planned**. Also include milestone dates where applicable.

4.1.1 Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change then installs the program into the production environment without testing).

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the Rules of Behavior. If they are incorporated in the Rules of Behavior reference the applicable section.

- Have all positions been reviewed for sensitivity level? If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- Indicate the level of screening required for privileged users and limited privilege users who can bypass security processes and controls. Include the number of privileged and limited privilege users.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

- Is user access restricted (least privilege) to data files, to processing capability, or to peripherals and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform the job?

- Are critical functions divided among different individuals (separation of duties) to ensure that no individual has all necessary authority or information access which could result in fraudulent activity?

- Is there a process for requesting, establishing, issuing, and closing user accounts?

- What mechanisms are in place for holding users responsible for their actions?

- What are the termination procedures for a friendly termination and an unfriendly termination?

4.1.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. Note: the explanation provided below is an excerpt from NIST Special Publication, *Generally Accepted Principles and Practices for Securing Information Technology Systems*.

4.1.2.1 Explanation of Physical and Environment Security

Access Controls. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server.

Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.

It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

Fire Safety Factors. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems.

Failure of Supporting Utilities. Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. Organizations should ensure that these utilities, including their many elements, function properly.

Structural Collapse. Organizations should be aware that a building may be subjected to a load greater than it can support. Most commonly this results from an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.

Plumbing Leaks. While plumbing leaks do not occur every day, they can be seriously disruptive. An organization should know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves) .

Interception of Data. Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

Mobile and Portable Systems. The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations should:

- Secure storage of laptop computers when they are not in use.

- Encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop computer is lost or stolen.

4.1.2.2 Computer Room Example

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all-inclusive or to imply that all systems should have all controls listed.

Example:
Physical/Environmental Controls for Computer Room

In Place
Card keys for building and work-area entrances
24-hour guards at all entrances/exits
Cipher lock on computer room door
Raised floor
Dedicated cooling system
Humidifier in tape library
Emergency lighting in computer room
Four fire extinguishers rated for electrical fires
One B/C-rated fire extinguisher
Smoke, water, and heat detectors
Emergency power-off switch by exit door
Surge suppression
Emergency replacement server
Zoned dry pipe sprinkler system
Uninterruptable power supply for LAN servers
Power strips/suppressers for peripherals
Power strips/suppressers for computers
Controlled access to file server room

Planned
Plastic sheets for water protection, August 1997
Closed-circuit television monitors, January 1998

4.1.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported in this section.

- User support. Is there a help desk or group that offers advice and can respond to security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, and report incidents and/or problems?

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.

- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.

- Audit trails for receipt of sensitive inputs/outputs.

- Procedures for restricting access to output products.

- Procedures and controls used for transporting or mailing media or printed output.

- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary, and Confidential).

- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).

- Audit trails for inventory management.

- Media storage vault or library physical and environmental protection controls and procedures.

- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).

- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.

- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

4.1.4 Contingency Planning

Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.

Briefly describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable and provide the detailed plans as an attachment. Include consideration of the following questions in this description:

- Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event? List the date it was last tested.

- Are tested disaster recovery plans in place for all supporting IT systems and networks?

- Are formal written emergency operating procedures posted or located to facilitate their use in emergency situations?

- How often are contingency, disaster, and emergency plans tested?

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls.

- Any agreements for backup processing (e.g., hotsite contract with a commercial service provider).

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).

- Location of stored backups (off-site or on-site).

- Generations of backups kept.

- Coverage of backup procedures, e.g., what is being backed up.

4.1.4.1 Application Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes. This helps ensure that only authorized software is installed on the system. Such controls may include a software configuration policy that grants managerial approval (re-authorize processing) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing illegal use of shareware or copyrighted software. Software maintenance procedures may also be termed version control, change management, or configuration management. The following questions are examples of items that should be addressed in responding to this section:

- Was the application software developed in house or under contract?
- Does the government own the software?
- Was the application software received from another federal agency with the understanding that it is federal government property?
- Is the application software a copyrighted commercial off-the-self product or shareware?
- If a copyrighted commercial off-the-self product (or shareware), were sufficient licensed copies of the software purchased for all of the systems on which this application will be processed?
- Is there a formal change control process in place for the application, and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data "live" data or made-up data?
- Are all changes to the application software documented?
- Are test results documented?
- How are emergency fixes handled?
- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Describe any reconciliation routines used by the system, i.e., checksums. Include a description of the actions taken to resolve any discrepancies.
- Are there organizational policies against illegal use of copyrighted software or shareware?

- Are periodic audits conducted of users' computers (PCs) to ensure only legal licensed copies of software are installed?

- What products and procedures are used to protect against illegal use of software?

- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

4.1.4.2 Data Integrity/Validation Controls

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected. The following questions are examples of some of the controls that fit in this category:

- Is virus detection and elimination software installed? If so, are there procedures for:
  - Updating virus signature files;
  - Automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan for macro viruses); and
  - Virus eradication and reporting?

- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.

- Are password crackers/checkers used?

- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? Techniques include consistency and reasonableness checks and validation during data entry and processing. Describe the integrity controls used within the system.
- Are intrusion detection tools installed on the system? Describe where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions. (Reference Section 5.MA.3 Production, Input/Output Controls if the procedures for handling intrusions are already described.)

- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?

- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?

- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission? State whether message authentication has been determined to be appropriate for your system. If so, describe the methodology.

4.1.4.3 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support system(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations.

List the documentation maintained for the application. The example list is provided to show the type of documentation that would normally be maintained for a system and is not intended to be all inclusive or imply that all systems should have all items listed.

Example Documentation for Major Application

- Vendor supplied documentation of hardware
- Vendor supplied documentation of software
- Application requirements
- Application program documentation and specifications
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Memoranda of understanding with interfacing systems
- Disaster recovery plans
- User rules of behavior
- User manuals
- Risk assessment
- Backup procedures
- Authorize processing documents and statement

4.1.5 Security Awareness and Training

The Computer Security Act requires federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user should be versed in acceptable rules of behavior for the application before being allowed access to the system. The training program should also inform the user on how to get help when having difficulty using the system and procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

Include in this section of the plan information about the following:

- The awareness program for the application (posters, booklets, and trinkets).

- The type and frequency of application-specific training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).

- The Rules of the System are discussed.

- How to detect and respond to suspected security incidents.

- How to get help in using the system and its security features.

- The type and frequency of training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).

- The procedures for assuring that employees and contractor personnel have been provided adequate training.

- Are system users trained about the HQ policies, procedures, and guidelines.

Note: Contractor employees are required to receive the same level of automated information systems security awareness and training as Federal employees. This training requirement should be included as appropriate in all contracts.

4.1.6 Incident Response Capability

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms. Computer security incidents are becoming more common and their impact far-reaching. When faced with an incident, an agency should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. OMB A-130 requires each agency to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. In this section, describe the incident handling procedures in place for the general support system. Areas of consideration include:

- Is there a formal incident response capability (in-house or external) available? If there is no capability established, is there a help desk or similar organization available for assistance?

  – Are there procedures for reporting incidents handled either by system personnel or externally?

  - Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?

- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?

- Identify the names and phone numbers of people who should be called if a security incident is discovered.

- What preventative measures are in place?
  - Intrusion detection tools
  - Automated audit logs
  - Penetration testing

4.2 Technical Controls

Technical controls are hardware and software controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations, and should be consistent with the management of security within the organization. Describe the technical control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application.

4.2.1 Identification and Authentication

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

4.2.1.1 Identification

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, describe how the major application identifies access to the system.

Unique Identification**.** An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

Correlate Actions to Users. The system should internally maintain the identity of all active users and be able to link actions to specific users. (See the section on audit trails.)

Maintenance of User IDs. An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.

Inactive User IDs. User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.

4.2.1.2 Authentication

Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and something the individual *is* (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

In this section, describe the major application’s authentication control mechanisms. Below is a list of items that should be considered in the description:

- Describe the method of user authentication (password, token, and biometrics).

- If a password system is used, provide the following specific information:

  - Allowable character set,
  - Password length (minimum, maximum),
  - Password aging time frames and enforcement approach,
  - Number of generations of expired passwords disallowed for use,
  - Procedures for password changes,
  - Procedures for handling lost passwords, and
  - Procedures for handling password compromise.

- Procedures for training users and the materials covered.

Note: The recommended minimum number of characters in a password is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).

- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.

- Describe any token controls used on the system and how they are implemented.

  - Are special hardware readers required?
  - Are users required to use a unique Personal Identification Number (PIN)?
  - Who selects the PIN, the user or System Administrator?
  - Does the token use a password generator to create a one-time password?
  - Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, and application).

- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.

- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).

- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.

- If digital signatures are used, the technology must conforms with FIPS 186, *Digital Signature Standard,* and FIPS 180, *Secure Hash Standard,* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures. Address the following specific issues:

  – State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted and the name and title of the official granting the waiver.

  – Describe the use of electronic signatures and the security control provided.

  – Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

4.2.2 Logical Access Controls (Authorization/Access Controls)

Logical access controls are the system-based mechanism used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). The following are areas that should be considered.

- Describe formal policies that define the authority that will be granted to each user or class of users. Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

- Identify whether the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the application's capability to establish an Access Control List, or register of the users and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.
- Describe policy or logical assess controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This

"discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for authentication, include this information in the section above.) If encryption is used as part of the access controls, provide information about the following:

  – What cryptographic methodology (e.g., secret key and public key) is used? If a specific off-the-shelf product is used, provide the name of the product. If it meets Federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

  – Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

- If your application is running on a system that is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

It is recommended that a standardized log-on banner be placed on the system. Public Law 99-474 requires that a warning message is displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and fines or imprisonment can punish unauthorized use. Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when P.L. 99-474 was enacted. Thus, due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements. In this section, describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

NASA requires that where applicable, the following standard warning banner be applied. Note if a banner similar to the following exists.

> WARNING:
>
> This is a U.S. GOVERNMENT COMPUTER This system is for use of authorized users only. By accessing and using the computer system, you are consenting to system monitoring, including the monitoring of keystrokes. Unauthorized use of, or access to, this computer may subject you to disciplinary action and criminal prosecution.

4.2.3 Public Access Controls

Where an agency's application promotes or permits public access, additional security controls are needed to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records.

Public access systems are subject to a greater threat from outside attacks. In public access systems, users are often anonymous and untrained in the system and their responsibilities. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public trust and confidence. Threats from insiders are also greater (e.g., errors introduced by disgruntled employees or unintentional errors by untrained users).

If the public accesses the major application, describe the additional controls in place. The following list describes the type of controls that might provide protection in a public access system and issues that should be considered. It is not intended to include all possible controls or issues.

- Some form of identification and authentication (this may be difficult)
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access "live" databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

4.2.4 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place. A list of items to consider are provided below:

- Does the audit trail support accountability by providing a trace of user actions?

- Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?

- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?

- Are audit trails used as online tools to help identify problems other than intrusions as they occur?

- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? In general, an event record should specify:

  - Type of event
  - When the event occurred
  - User ID associated with the event
  - Program or command used to initiate the event.

- Is access to online audit logs strictly controlled?

- Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?

- Describe how frequently audit trails are reviewed and whether there are review guidelines.

- Can the audit trail be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information?

- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

- Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be used in a real-time, or near real-time fashion. Does the organization use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data?

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

4.2.5 Information Technology Security Review

An *Information Technology Security Review* should be performed by the Code CI-1 IT Security Group for each major application, and attached to the Security Plan. **Appendix E** contains an example of the type of information that is asked for during the review. The IT Security Group maintains a copy of the review in a database.

5. General Support System Format

This portion of the Security Plan is for a general support system, and is divided into two main sections, being Operational and Technical Controls.

5.1 Operational Controls

The operational controls address security mechanisms that focus on methods that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. Describe the operational control measures (i**n place** or **planned**) that are intended to meet the protection requirements of the general support system.

5.1.1 Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the Rules of Behavior. If they are incorporated in the Rules of Behavior, reference the applicable section .

- Have all positions have been reviewed for sensitivity level? If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- Indicate the level of screening required for privileged users and limited privilege users who can bypass security processes and controls. Include the number of privileged and limited privilege users.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

- Are user’s access restricted (least privilege) to data files, to processing capability, or to peripherals and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform the job?

- Are critical functions divided among different individuals (separation of duties) to ensure that no individual has all necessary authority or information access which could result in fraudulent activity?

- Is there a process for requesting, establishing, issuing, and closing user accounts?

- What mechanisms are in place for holding user’s responsible for their actions?

- What are the termination procedures for a friendly termination and an unfriendly termination?

5.1.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place or planned for the general support system.

5.1.2.1 Explanation of Physical and Environment Security

Access Controls. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server.

Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.

It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

Fire Safety Factors. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems.

Failure of Supporting Utilities. Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. Organizations should ensure that these utilities, including their many elements, function properly.

Structural Collapse. Organizations should be aware that a building may be subjected to a load greater than it can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.

Plumbing Leaks. While plumbing leaks do not occur every day, they can be seriously disruptive. An organization should know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves) .

Interception of Data. Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

Mobile and Portable Systems. The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations should:

- Secure storage of laptop computers when they are not in use.

- Encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop computer is lost or stolen.

5.1.2.2 Computer Room Example

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all inclusive or to imply that all systems should have all controls listed.

Example of Physical/Environmental Controls
For Computer Room

In Place
Card keys for building and work-area entrances
24-hour guards at all entrances/exits
Cipher lock on computer room door
Raised floor in computer room
Dedicated cooling system
Humidifier in tape library
Emergency lighting in computer room
Four fire extinguishers rated for electrical fires
One B/C rated fire extinguisher
Smoke, water, and heat detectors
Emergency power-off switch by exit door
Surge suppresser
Emergency replacement server
Zoned dry pipe sprinkler system
Uninterruptable power supply for LAN servers
Power strips/suppressers for peripherals
Power strips/suppressers for computers
Controlled access to file server room

Planned
Plastic sheets for water protection, August 1997
Closed-circuit television monitors, January 1998

5.1.2.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the general support system. Below is a sampling of topics that should be reported in this section.

- User support.

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.

- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.

- Audit trails for receipt of sensitive inputs/outputs.

- Procedures for restricting access to output products.

- Procedures and controls used for transporting or mailing media or printed output.

- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary, and Confidential).

- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).

- Audit trails for inventory management.

- Media storage vault or library physical and environmental protection controls and procedures.

- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).

- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.

- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

5.1.3 Contingency Planning

General support systems require appropriate emergency, backup, and contingency plans. These plans should be tested regularly to assure the continuity of support in the event of system failure. Also, these plans should be known to users and coordinated with their plans for applications.

Describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster should occur and provide a reference to the detailed plans. Include consideration of the following questions in this description:

- Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event? List the date it was last tested.

- Are tested disaster recovery plans in place for all supporting IT systems and networks?

- Is formal written emergency operating procedures posted or located to facilitate their use in emergency situations?

- How often are contingency, disaster, and emergency plans tested?

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls.

- Any agreements for backup processing (e.g., hot site contract with a commercial service provider).

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).

- Location of stored backups (off-site or on-site).

- Generations of backups kept.

- Coverage of backup procedures, e.g., what is being backed up.

5.1.3.1 Hardware and System Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, hardware, operating system software, and other software to ensure that the hardware and software function as expected, and that a historical record is maintained of application changes. These controls may also be used to ensure that only authorized software is installed on the system. Such controls may include a hardware and software configuration policy that grants managerial approval (re-certification and re-accreditation) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing, illegal use of shareware or copyrighted software. The following questions are examples of items that should be addressed in responding to this section:

- Are procedures in place to ensure that maintenance and repair activities are accomplished without adversely affecting system security? Consider the following items:

  – Restriction/controls on those who perform maintenance and repair activities.

  – Special procedures for performance of emergency repair and maintenance.

- – Management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.

- – Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).

- – Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.

Describe the configuration management procedures for the system. Consider the following items in the description:

- Version control that allows association of system components to the appropriate system version.

- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.

- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.

- Change identification, approval, and documentation procedures.

- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.

- Are test data "live" data or made-up data?

- How are emergency fixes handled?

Describe the policies for handling copyrighted software or shareware. Consider including in this description answers to the following questions:

- Are there organizational policies against illegal use of copyrighted software or shareware?

- Do the policies contain provisions for individual and management responsibilities and accountability, including penalties?

- Are periodic audits conducted of users' computers (PCs) to ensure only legal licensed copies of software are installed?

- What products and procedures are used to protect against illegal use of software?

- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

5.1.3.2 Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected. The following questions are examples of some of the controls that fit in this category:

- Is virus detection and elimination software installed? If so, are there procedures for:
  - Updating virus signature files;
  - Automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan
  - for macro viruses); and
  - Virus eradication and reporting?

- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.

- Are password crackers/checkers used?

- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? Techniques include consistency and reasonableness checks and validation during data entry and processing. Describe the integrity controls used within the system.

- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?

- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission? State whether message authentication has been determined to be appropriate for your system. If so, describe the methodology.

5.1.3.3 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures.

List the documentation maintained for the general support system. An example list is provided to show the type of documentation that would normally be maintained for a system and is not intended to be all-inclusive or imply that all systems should have all items listed.

Examples of General Support System Documentation

- Vendor supplied documentation of hardware
- Vendor supplied documentation of software
- General support system security plan
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Disaster recovery plans
- User rules/procedures
- User manuals
- Risk assessment
- Backup procedures
- Authorize processing documents and statements

5.1.4 Security Awareness and Training

The Computer Security Act requires federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user should be versed in acceptable rules of behavior for the system before being allowed access to the system. The training program should also inform the user on how to get help when having difficulty using the system and procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

Include in this section of the plan information about the following:

- The awareness program for the system (posters, booklets, and trinkets).

- The type and frequency of system-specific training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).

- The Rules of the System are discussed.

- The procedures for assuring that employees and contractor personnel have been provided adequate training.

- If system users trained about the HQ policies, procedures, and guidelines.

Note: Contractor employees are required to receive the same level of automated information systems security awareness and training as federal employees. This training requirement should be included as appropriate in all contracts.

5.1.5 Incident Response Capability

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms. Computer security incidents are becoming more common and their impact far-reaching. When faced with an incident, an agency should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. OMB A-130 requires each agency to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. In this section, describe the incident handling procedures in place for the general support system. Areas of consideration include:

- Is there a formal incident response capability (in-house or external) available? If there is no capability established, is there a help desk or similar organization available for assistance?

  - Are there procedures for reporting incidents handled either by system personnel or externally?

  - Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?

- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?

- Identify the names and phone numbers of people who should be called if a security incident is discovered.

- What preventative measures are in place?
  - Intrusion detection tools
  - Automated audit logs
  - Penetration testing

5.2 Technical Controls

Technical controls are hardware and software controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. In this section, describe the technical control measures (**in place** or **planned**) that are intended to meet the protection requirements of the general support system.

5.2.1 Identification and Authentication

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

5.2.1.1 Identification

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, describe how general support system identifies access to the system.

Unique Identification**.** An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

Correlate Actions to Users. The system should internally maintain the identity of all active users and be able to link actions to specific users. (Refer to the section on Audit Trails.)

Maintenance of User IDs. An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.

Inactive User IDs. User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.

5.2.1.2 Authentication

Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and something the individual *is* (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

In this section, describe the general support system’s authentication control mechanisms. Below is a list of items that should be considered in the description:

- Describe the method of user authentication (password, token, and biometrics).

- If a password system is used, provide the following specific information:

  – Allowable character set,
  – Password length (minimum, maximum),
  – Password aging time frames and enforcement approach,
  – Number of generations of expired passwords disallowed for use,
  – Procedures for password changes,
  – Procedures for handling lost passwords, and
  – Procedures for handling password compromise.

- Procedures for training users and the materials covered.

Note: The recommended minimum number of characters for a password is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).

- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.

- Describe any token controls used on this system and how they are implemented.

  – Are special hardware readers required?
  – Are users required to use a unique Personal Identification Number (PIN)?
  – Who selects the PIN, the user or System Administrator?
  – Does the token use a password generator to create a one-time password?
  – Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, and application).

- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.

- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).

- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.

- If digital signatures are used, the technology must conforms with FIPS 186*, Digital Signature Standard* and FIPS 180, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures. Address the following specific issues:

  - State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted, and the name and title of the official granting the waiver.

  - Describe the use of electronic signatures and the security control provided.

  - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

5.2.2 Logical Access Controls (Authorized/Access Controls)

Logical access controls are the system-based mechanism used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the general support system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). The following are areas that should be considered.

- Describe formal policies that define the authority that will be granted to each user or class of users. Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

- Identify whether the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the system's capability to establish an Access Control List or register of the users, and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This "discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for authentication, include this information in the section above.) If encryption is used as part of the access controls, provide information about the following:

  – What cryptographic methodology (e.g., secret key and public key) is used? If a specific off-the-shelf product is used provide the name of the product. If it meets Federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

  – Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

- If the general support system is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

In addition, documentation for a system should include a standardized log-on banner. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and fines or imprisonment can punish unauthorized use. Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when P.L. 99-474 was enacted. Thus, due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements. In this section, describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

NASA requires that where applicable, the following standard warning banner be applied. Note if a banner similar to the following exists.

> WARNING:
>
> This is a U.S. GOVERNMENT COMPUTER This system is for use of authorized users only. By accessing and using the computer system, you are consenting to system monitoring, including the monitoring of keystrokes. Unauthorized use of, or access to, this computer may subject you to disciplinary action and criminal prosecution.

5.2.3 Public Access Controls

Where an agency's application promotes or permits public access, additional security controls are needed to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records.

Public access systems are subject to a greater threat from outside attacks. In public access systems, users are often anonymous and untrained in the system and their responsibilities. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public trust and confidence. Threats from insiders are also greater (e.g., errors introduced by disgruntled employees or unintentional errors by untrained users).

If the public accesses the major application, describe the additional controls in place. The following list describes the type of controls that might provide protection in a public access system and issues that should be considered. It is not intended to include all possible controls or issues.

- Some form of identification and authentication (this may be difficult)
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures

- CD-ROM for on line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access "live" databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

5.2.4 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place. A list of items to consider are provided below:

- Does the audit trail provide accountability by providing a trace of user actions?

- Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?

- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?

- Are audit trails used as online tools to help identify problems other than intrusions as they occur?

- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify:

  - Type of event
  - When the event occurred
  - User ID associated with the event
  - Program or command used to initiate the event.

- Is access to online audit logs strictly controlled?

- Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?

- Describe how frequently audit trails are reviewed and whether there are review guidelines.

- Can the audit trail be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

- Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be used in a real-time, or near real-time, fashion. Does the organization use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data?

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

5.2.5 Information Technology Security Review

An *Information Technology Security Review* should be performed by the Code CI-1 IT Security Group for each major application, and attached to the Security Plan. **Appendix E** contains an example of the type of information that is asked for during the review. The IT Security Group maintains a copy of the review in a database.

Appendix A - Terms

Acceptable Risk	A risk that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Accreditation	The authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security.
Acquisition Specifications	Appropriate technical, administrative, physical and personnel security requirements should be specified and are to be included in the specifications for the acquisition or operations of information technology installations, equipment, software, systems and related services.
Adequate Security	Security commensurate with the risk and magnitude of information. Includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
Application	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Assign Responsibility for Security	Assign responsibility in each system to an individual knowledgeable in the information technology used in the system and for providing security for such technology.
Audit and Variance Detection	Controls should be in place to allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.
Audit Trails Mechanism	An automated mechanism should be operational to provide a system monitoring and recording capability to retain a chronological record of system activities so that all security relevant events can be traced to a specific client for accountability.
Authorization and Access Controls	The system should employ hardware and software features to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and limit access to programming resources, and/or to detect unauthorized activities.
Authorize Processing	Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be reauthorized at least every three years.
Awareness Training	Includes: awareness programs set the stage for training by changing organizational attitudes toward realization that the importance of security and the adverse consequences of its failure; the purpose of training is to teach the skills that will enable them to perform their jobs

	more effectively; and education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.
Certification	The technical evaluation that establishes the extent to which a computer system, application or network design and implementation meets a pre-specified set of security requirements.
Computer Viruses	All NASA offices will comply with the established procedures for detecting and eliminating viral infections from NASA IT computers and PCs. If viruses are detected or suspected, they are to be reported immediately to the HELPDESK (XXX-XXXX).
Confidentiality Controls	Controls should provide protection for data that must be held in confidence and from unauthorized disclosure. Providing data protection at the user site, the computer facility, in transit, or some combination of these can be ensured by some form of encryption.
Contingency and Disaster Recovery Plans	Contingency and disaster recovery plans should be established, maintained and tested to prevent loss of information, minimize down time, and provide reasonable continuity of computer and network services if normal system operations are interrupted.
Continuity of service	The agency should assure that in case of an interruption to operation of the system, there is an ability to recover and provide services sufficient to meet the minimal needs of users of the system.
Controls Over the Security of Applications	Controls should be in place to ensure that the security of an application does not compromise the security of other applications running on that system. General support system managers should be knowledgeable about the risk each application presents to the overall system.
Designated Approving Authority	Senior management official who has the authority to authorize processing (accredit) an automated information major application or general support system and accept the risk associated with the system.
Documentation	Descriptions of the hardware/software policies and procedures related to the computer security of the network, descriptions of the network layout, software, hardware, and configuration or cable charts should be available for those who need them.
General Support System	An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shred information processing service organization.
Individual Accountability	Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Integrity Controls	Controls should be in place to protect the system and data from accidental or malicious alteration or destruction, and provide assurance to the user that data has not been altered.
Major Application	An application that requires special attention to security due to the risk

	and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Personnel Screening	Personnel screening should be in place. Appropriate screening should be conducted for NASA employees and contractors who participate in managing, designing, developing, operating, or maintaining computer systems processing sensitive or mission-critical information, or who access automated sensitive or mission-critical information. The screening shall be commensurate with the sensitivity, criticality, or value of the information to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual.
Personnel Security	All direct hire corporate employees are subject to reference checks prior to employment. Those individuals occupying positions with a higher level of security designation may be subject to additional background checks. All employees and long term contractors will be issued XXXXXXXXXXXXXX. Visitors will be escorted at all times.
Physical and Environmental Protection	Physical and environmental protection should be in place for all IT installations. This should include protections against a wide variety of physical and environmental threats and hazards including deliberate intrusions, utility outages and breakdowns. This includes the installation of appropriate devices such as fire extinguishers, locks, or video cameras.
Physical Security	The operational areas of major computer installations, including LAN file servers, will be designated as controlled and restricted areas in which access is not permitted unless specifically authorized. Other areas such as telephone and wiring closets, environmental controls, power and system closets, and supply storage areas will also be secured.
Production Input and Output Controls	Formal procedures for handling of input data by properly screened persons and for maintaining an audit trail should be prepared. Printouts and storage media should be identified as to content and sensitivity and sensitive/critical data media should be securely stored. Data media and storage containing sensitive data should be overwritten before it is released outside the original owner's control.
Production, Input/Output Controls	Controls in place that provide for proper handling, processing, storage and disposal of the input and output of the network. Procedures for handling of input data by properly screened persons and for maintaining an audit trail should be prepared. Printouts and storage media should be identified as to content and sensitivity and sensitive/critical data media should be securely stored. Data media and storage containing sensitive data should be overwritten before it is released outside the original owner's control.
Review of Security Controls	Review the security controls in each system when significant modifications are made to the system, but at least every three years.
Risk	The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.
Risk Assessments	A risk management policy ensures that the balance of risks,

	vulnerabilities, threats, and countermeasures achieves a residual level of risk that is acceptable based on the sensitivity or criticality of the individual IT system. Periodic risk assessments must be conducted for new and existing systems to assure that appropriate, cost-effective protective measures are incorporated and are commensurate with the sensitivity, criticality, and value of associated computer systems, computer applications, and information processed. Risk assessments should be performed prior to the construction or operational use of a system, when there is a significant change to an existing system, at periodic intervals commensurate with the sensitivity/criticality of the information processed but not greater than five (5) years.
Rules	Includes the set of rules of behavior that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Security Awareness and Training	A security awareness and training program should be established to ensure that employees, contractors, and volunteer personnel are aware of their security responsibilities and how to fulfill them. The program should include new employee security briefings, annual refresher training, and training for information technology and security personnel.
Security Awareness and Training	The established security awareness and training programs will ensure that employee, contractor, and volunteer personnel as well as new employees are aware of their security responsibilities and how to fulfill them. The program will include new employee security briefings, annual refresher training, and additional training for information technology and security personnel.
Security Testing	Sensitive/Critical automated information systems that are under development should be reviewed to ensure that security tests are scheduled and conducted within the proposed general support environment. System tests are required before sensitive/automated critical automated information systems are certified and placed in operational use.
System Security Plan	Plan for adequate security of each general support system as part of the organization’s Information Resources Management (IRM) planning process. The security plan shall present in place and planned controls for the system. The security plan (for general support systems) shall include rules of the system and provisions for training, personnel controls, incident response capability, continuity of support, technical security, and management authorization for system interconnection.
Technical Controls	Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.
Threat	An activity, deliberate or unintentional, with the potential for causing

	harm to an automated information system or activity.
User Identification and Authentication	Controls must be in place to verify the identity of a station, originator, or individual before allowing access to the system or specific categories of information within the system. The controls may also be used to verify that only authorized persons are performing certain processing activities on the system. These controls include the use of passwords, tokens, or other personal mechanism to authenticate an identity.
Vulnerability	A flaw or weakness that may allow harm to occur to an automated information system or activity.

Appendix B - Policy Definitions

Federal Legislation

Computer Fraud and Abuse Act of 1986 (18 USC 1030)
Addresses the criminal aspects of the unauthorized access and/or use of US Government computers.

Computer Matching and Privacy Act of 1988 (PL 100-503)
To ensure privacy, integrity and verification of data disclosed for computer matching. To establish Data Integrity Boards within federal agencies.

Computer Security Act of 1987 (40 USC 759) (PL 100-235)
Makes National Institute of Standards and Technology (NIST) responsible for security guidelines for information systems. Defines terms such as computer systems, sensitive information, and federal agencies. Federal agencies mandated to prepare security plans for NIST and NSA for review. Requires mandatory periodic computer security training for all levels of federal agency personnel.

Electronic Communications Privacy Act of 1986 (18 USC 2510, Suppl. 4, 1986)
Defines terms such as electronic communications and privacy. Defines the unauthorized interception of an electronic communication as a crime, as well as an invasion of an individual's right to privacy that will subject an offender to civil liabilities and damages.

Federal Manager's Financial Integrity Act (31 USC 1352)
Requires that the head of each department or agency establish and maintain an Internal Controls program having the capability to assess the adequacy of measures that safeguard information system resources.

Privacy Act of 1974 (5 USC 522a) (PL 93-579)
Mandates that all Federal agencies maintaining personal information employ appropriate physical, technical, and administrative safeguards to ensure the confidentiality of records and to protect against threats or hazards. Agencies must prevent situations which could cause substantial harm, embarrassment, inconvenience, or unfair treatment to any individual or entity on whom information is maintained.

Presidential Directives and Executive Orders

National Security Directive 42 (NSD 42) - *National Policy for the Security of National Security Telecommunications and Information Systems*
Establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems.

National Security Decision Directive 145 (NSDD 145) *National Policy on Telecommunications and Automated Information Systems Security*
Mandates the protection of both classified and sensitive information, and created a federal interagency structure for computer security.

Executive Order 12958 - *Classified National Security Information*
This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. (supersedes E.O. 12356, *National Security Information)*

National Security Policy

National Security Decision Directive 145 (NSDD 145)
National Policy on Telecommunications and Automated Information Systems Security
Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding systems that process, store, or communicate sensitive information. Establishes a mechanism for policy development. Assigns implementation responsibilities.

National Telecommunications and Information System Security Policy (NTISSP) 200
National Policy on Controlled Access Protection
Requires a minimum technical C2 level of protection for AIS accessed by more than one user.

NTISSP 300 - *National Policy on Control of Compromising Emanations*
Requires departments and agencies to plan, implement, and manage TEMPEST emanations control programs.

NTISSP 500 - *Information Systems Security Education, Training, and Awareness*
Establishes the requirement for departments and agencies to develop and implement Telecommunications and Automated Information System Security (TAISS) programs to enhance awareness of all levels of employees.

National Telecommunications and Information System Security Instruction (NTISSI) 4001 - *Controlled Cryptographic Items*
Established new categories of secure telecommunications and information handling equipment and associated cryptographic components.

Federal Information Processing Standards

FIPS PUB 41 - *Computer Security Guidelines for Implementing the Privacy Act of 1974*
Provides guidance for organizations that are selecting methods for protecting personal data in computer systems.

FIPS PUB 73 - *Guidelines for Security of Computer Applications*
Contains a discussion of security objectives for computer systems and describes such controls as data validation, user identity verification, authorization, journaling, variance detection, and encryption.

FIPS PUB 74 - *Guidelines for Implementing and Using the NBS Data Encryption Standard*
Contains guidance for the use of Data Encryption Standard.

FIPS PUB 83 - *Guideline on User Authentication Techniques for Computer Network Access Control*
Contains guidance for the selection and implementation of authentication techniques for remote terminal users. Describes such techniques as passwords, identification tokens, verification by personal attributes, identification of remote devices, encryption, and computerized authorization techniques.

FIPS PUB 88 - *Guideline on Integrity Assurance and Control in Database Administration*
Contains advice for achieving database integrity and security control.

FIPS PUB 102 - *Guideline for Computer Security Certification and Accreditation*
Contains guidance for setting up and executing a computer certification and accreditation program. Includes descriptions of evaluation techniques and issues commonly faced by personnel developing a program.

FIPS PUB 112 - *Standard on Password Usage*
Contains a discussion of factors to consider in designing, implementing, and using access control systems based on passwords. Specifies a range of recommendations for systems at different levels of security.

FIPS PUB 113 - *Standard on Computer Data Authentication*
Contains the specification for the Data Authentication Algorithm (DAA), which automatically and accurately detects intentional and accidental unauthorized modification. The DAA is based on DES.

FIPS PUB 140 - *General Security Requirements for Equipment Using the Data Encryption Standard*
Contains security requirements for implementing the DES in telecommunications equipment.

Office of Management and Budget

OMB Circular A-130 - *Management of Federal Information Resources*
Established requirements for effective and efficient management of federal information resources. Requires all agency information systems to provide a level of security commensurate with the sensitivity of the information, the risk of its unauthorized access, and the harm that could result from improper access. Also, requires all agencies to establish security programs to safeguard the sensitive information that they process.

OMB Bulletin No. 90-08 - *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*
The OMB Bulletin 90-08 discuses what a security plan should include. This bulletin is in effect until NIST revises the plan.

OMB Circular A-127 - *Financial Management Systems*
Established a program to assure the integrity of federal financial management systems.

OMB Circular A-123 - *Internal Control Systems*
Directed agency heads and managers to set up management plans and to take responsibility for eliminating fraud, waste, and abuse in government programs.

Other Important Security Related Documents

The Director of Central Intelligence Directive 1/16 (DCID 1/16)
Establishes security standards for foreign intelligence information, including sensitive compartmental information (SCI) processed, transmitted or handled by an information system.

Federal Personnel Manual
Requires AIS positions be designated in terms of sensitivity to assure that personnel hired for these positions are appropriately screened.

The Rainbow Series
Published by the National Computer Security Center's Technical Guidelines Program; includes the Trusted Computer System Evaluation Criteria (Orange Book). Other publications in the series provide detailed interpretations of certain Orange Book requirements.

NASA Computer Security Related Documents

HQMI 2410.2A - *NASA Headquarters Management Instruction: Assuring the Security and Integrity of NASA Headquarters Automated Information Resources*

HQPG 1590.1 - *Headquarters Operations Services Guide*

NHB 1620.3C - *NASA Security Handbook*

NPG 2810 - NASA Procedures and Guidance for the Security of Information Technology.

NMI 2410.10B - *NASA Management Instruction: NASA Software Management, Assurance, and Engineering Policy*

NASA Headquarters Information Technology Security Policies

Appendix C - Rules of Behavior: Major Application

HYPOTHETICAL GOVERNMENT AGENCY’S (HGA)
FINANCIAL INFORMATION SYSTEM

1. Introduction

The following rules of behavior are to be followed by all users of the HGA’s Financial Information System (HFIS). The rules clearly delineate responsibilities of and expectations for all individuals with access to the HFIS. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2. Responsibilities

The Information Systems Security Office (ISSO) is responsible for ensuring an adequate level of protection is afforded information systems, through an appropriate mix of technical, administrative, and managerial controls. The ISSO develops policies and procedures, develops and conducts user and contractor awareness sessions, and conducts inspections and spot checks to determine that an adequate level of compliance with security requirements exists. The office periodically conducts vulnerability analyses to help determine if security controls are adequate, given the ever-changing nature of the information systems environment. Special attention must be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in HGA’s security posture.

3. Other Policies and Procedures

The rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing HFIS. The rules are consistent with the policy and procedures described in the following directives:

HGA IRM Computer Security Handbook. The newly revised Handbook dated April 4, 1998, contains computer security guidance on a wide range of topics, i.e., personnel security, incident handling, access control mechanisms. This document contains responsibilities for the ISSO, HGA managers, and users.

HFIS Access Control Management Directive. This directive dated May 6, 1997, contains responsibilities for HFIS data owners and application administrators.

Draft HFIS Access Control Management Directive. The draft HFIS Access Control Management Directive contains specific responsibilities for the ISSO.

Letter for External (non-HGA) Users. A letter for Non-HGA users which transmits the applicable HGA policies should be provided to all non-HGA users while using HFIS, or when using HGA systems and applications in general. These responsibilities should be included in training HGA provides for agency security points of contact, and should be included in interagency agreements or other formal agreements or documents between HGA and other organizations.

4. Application Rules

4.1 Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work at home arrangement should:

- Be in writing;
- Identify the time period the work at home will be allowed;
- Identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;
- Identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the ISSO; see Section 4.2); and
- Be reviewed by HGA's personnel office prior to commencement.

4.2 Dial-in access. The IRM Division Director may authorize dial-in access to HFIS. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the ISSO will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords. If dial-in access is allowed to other applications on the system on which HFIS resides, the managers of those applications should also determine if such access could pose a risk to HFIS data.

4.3 Connection to the Internet. Some HGA personnel have access to the Internet. HGA should ensure that the user authentication required for access is adequate to protect HFIS programs and data. If such access is allowed, HGA should carefully document all external connections to ensure access to HFIS is limited to controlled points of entry.

4.4 Protection of software copyright licenses. All copyright licenses associated with the COTS HFIS software are complied with by HGA personnel, as well as by contractors responsible for developing and maintaining HFIS. HGA requires that all copyright licenses for all PC-based and LAN-based software used by HFIS program personnel and contractor personnel are understood and that these personnel comply with the license requirements. End users, supervisors, and function managers are ultimately responsible for this compliance.

4.5 Unofficial use of government equipment. Users should be aware that personal use of information resources is not authorized.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HFIS.

________________________________ ___________
Signature of User Date

Appendix D - Rules of Behavior: General Support System

Hypothetical Government Agency's (HGA)
Backbone Local Area Network

The rules of behavior contained in this document are to be followed by all users of the HGA Local Area Network (LAN). Users will be held accountable for their actions on the LAN. If an employee violates HGA policy regarding the rules of the LAN, they may be subject to disciplinary action at the discretion of HGA management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work at home arrangement should:

1. Be in writing;

2. Identify the time period the work at home will be allowed;

3. Identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;

4. Identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the ISSO; see Dial-in access section below); and

5. Be reviewed by HGA's personnel office prior to commencement.

Dial-in access. No dial-in access is used to access LAN servers. However, if a justifiable need occurs, the IRM Division Director may authorize dial-in access to a LAN server. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the ISSO will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one time passwords.

Connection to the Internet. Some HGA personnel have access to the Internet. Access to the Internet should be closely controlled by the ISSO. HGA divisions and staff managers and technicians should know that only HGA-authorized Internet connections will be allowed, and that all connections must conform to HGA's security and communications architecture.

Protection of copyright licenses (software) – LAN and PC users are not to download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

Unofficial use of government equipment – Users should be aware that personal use of information resources – LAN and PC – is not authorized.

Use of passwords – Users are to use passwords of a length specified by the LAN system administrators – a mix of six (6) to eight (8) alpha and numeric characters, they are to keep passwords confidential, and are not to share passwords with anyone.

System privileges – Users are given access to the LAN based on a need to perform specific work. Users are to work within the confines of the access allowed, and are not to attempt access to systems or applications to which access has not been authorized.

Individual accountability – Users will be held accountable for their actions on the LAN. This is stressed during computer security awareness training sessions

Restoration of service – The availability of the LAN is a concern to all users. All users are responsible for ensuring the restoration of services in the event the LAN is unoperational.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HGA Backbone LAN.

______________________________ __________

Signature of User Date

Appendix E - Information Technology Security Review

The following is an example of the Information Technology Security Review. This form is completed by the Code CI-1 IT Security Group, and is required for both Major Applications and General Support Systems.

Description: *		Version:
Purpose:		
Users: _ Single-user _ Work-group _ Code _ HQ _ Agency _ Partners _ Public		
NASA Owner:	Phone:	Code:
Requirement:		
Proposal:		
New Hardware: _ None _ New capability _ Add. capacity _ Life-cycle replacement		
Hardware type:	OS:	Name:
_ New procurement _ Excess re-use	_ Already baselined _ Being baselined	
Proposed physical location:	Network: _ Unsecured _ Public _ Private	
Privileged accounts:		
Changed Hardware: _ None _ NC _ AC _ LR	Baseline affected: _ Yes _ No	
Summary:		
Hardware type:	OS:	Name:
Current physical location:	Network: _ Unsecured _ Public _ Private	
Privileged accounts:		
Migrating Hardware: _ None		
Hardware type:	OS:	Name:
Current physical location:	Network: _ Unsecured _ Public _ Private	
Proposed physical location:	Network: _ Unsecured _ Public _ Private	
Privileged accounts:		
New Software: _ None _ New capability _ Enhancement _ Vendor support-ability		
Summary:		
Host name:	OS:	Network: _ Unsecured _ Public _ Private
Proposed physical location:	Technical POC:	
Why this host?		
Co-located systems:		
Privileged accounts:		
Changed Software: _ None _ NC _ E _ VS	Baseline affected: _ Yes _ No	
Summary:		
Host name:	OS:	Network: _ Unsecured _ Public _ Private
Current physical location:	Technical POC:	
Co-located systems:		
Privileged accounts:		
Migrating Software: _ None		
Current host:	OS:	Network: _ Unsecured _ Public _ Private
Proposed host:	OS:	Network: _ Unsecured _ Public _ Private
Proposed physical location:	Technical POC:	

Co-located systems:

Privileged accounts:

Security: Data categories (from NPD 2810):
_ MSN (*sensitive* Mission information)
_ BRT (*sensitive* Business and Restricted Technology information)
_ SER (*sensitive* Scientific, Engineering, and Research information)
_ ADM (*sensitive* Administrative information)
_ PUB (*non-sensitive* Public Access information)

Confidentiality requirement: _ None _ Standard _Above-standard

Integrity requirement: _ Standard _Above-standard

Availability requirement: _ Class I (Boeing admin.) _ 'A' List (2 hr response, 24x5)
_ Class II (Cust. admin.) _ Regular (4 hr resp., M-F 7:30-4)
_ Class not specified _ Maintenance not specified

Non-repudiation requirement: _ None

Client implementation: _ No dedicated client _ SMS push _ Login script _ Blast
_ WinInstall script (pulled) _ Manual install

User authentication: _ (n/a) _ Clear-text password _ Encrypted password
_ Software token _ Hardware token (SecurID)

OS Admin authentication: _ Clear-text password _ Encrypted password
_ Software token _ Hardware token (SecurID)

APP Admin authentication: _ Clear-text password _ Encrypted password
_ Software token _ Hardware token (SecurID)

Will data be exchanged in the clear? _ No _ Non-sensitive only _ Private Network only

Are multi-level user privileges required, e.g. read/write, read-only? _ No _ Yes

Additional security requirements/comments: _ None

Security requirements validated by:

Occasion: _Con _Doc _CR _SRR _PDR _CDR _DRR _TRR _ ORR _MRR _CCB

Project POC: *	Phone:	Org:
Security analyst:	Start date: *	Req'd date: *

Checklists: (C = complete, N = not applicable, P = planned)
C N P - Passed SEF interoperability testing (SEF)
C N P - Passed ISS scan (NOC)
C N P - Passed script review (ENG)

C N P - Passed site audit (SEC)
C N P - Required a firewall rule set change (ENG)
C N P - Meets applicable NASA HQ security procedures and guidelines (SEC)
C N P - Displays an appropriate warning banner (ENG)
C N P - Conforms to all Headquarters policies (SEC)

Significant Protection Mechanisms:

Unmitigated Risk: _ None

Recommendation: _ Approve _ Disapprove _ Approve with open work:

Signatures: (↓ always required ↓)	(↓ ORR / MRR / CCB only ↓)
Boeing IT Security: ___________________	Technical POC: _____________________
NASA IT Security: ___________________	NASA Owner: _____________________

Appendix F - Planned/Recommended Issues

Use this appendix to compile all of the planned items discussed throughout this document, as well as items that need attention.